NAVAL POSTGRADUATE SCHOOL
Monterey, California

AD-A275 638

DTIC
S ELECTE
FEB 1 4 1994
C **D**

THESIS

SECURITY ASPECTS OF COMPUTER
SUPPORTED COLLABORATIVE WORK

by

George V. Haroutunian, Jr.

September 1993

Thesis Advisor: Tung X. Bui
Associate Advisor: Roger Stemp

Approved for public release; distribution is unlimited

9 4 2 10 24 6

DTIC QUALITY INSPECTED 2

REPORT DOCUMENTATION PAGE

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 1993	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE
Security Aspects of Computer Supported Collaborative Work

5. FUNDING NUMBERS

6. AUTHOR(S)
George Van Haroutunian, Jr.
LCDR, SC, USN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 92943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release.
Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Computer Supported Collaborative Work (CSCW) is a topic of considerable academic inquiry and rapid commercial development. Meeting Room Systems, Conferencing Systems, Co-authoring and Argumentation Systems, Message Systems and Autonomous Agents which support group collaboration currently exist; however, Department of Defense (DoD) computer security requirements as they impact CSCW systems design has received little attention. This thesis describes CSCW systems and relates group dynamic issues to predict the form of the sophisticated CSCW which will probably become commonplace in the future. Next the Trusted Computer Security Evaluation Criteria (TCSEC) with which all DoD systems must comply are synopsized. An extension of the Bell-LaPadula model underlying the TCSEC requirements is proposed which would allow "Functionally Trusted CSCW" (FT-CSCW), CSCW which would meet many but not all of the TCSEC requirements. Possible first order (efficiency) effects of FT-CSCW, including the effect of sparse group domains, the breakdown of compartmentation, and organizational stratification are discussed. Second order (social) effects are also discussed, as are possible FT-CSCW problems (unstable group membership, attempts to implement Quality Improvement Circles, inter-group CSCW and the effect of visitors.) Finally, some suggestions are made for future FT-CSCW research.

14. SUBJECT TERMS
CSCW, Groupware, Computer Security

15. NUMBER OF PAGES
88

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

i

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18

Security Aspects of Computer Supported Collaborative Work

by

George V. Haroutunian, Jr.
Lieutenant Commander, Supply Corps, United States Navy
B.S., Florida State University, 1974

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1993

Author: _____
George V. Haroutunian, Jr.

Approved by: _____
Tung X. Bui, Thesis Advisor

_____
Roger Stemp, Associate Advisor

_____
David R. Whipple, Chairman
Department of Administrative Sciences

ii

ABSTRACT

Computer Supported Collaborative Work (CSCW) is a topic of considerable academic inquiry and rapid commercial development. Meeting Room Systems, Conferencing Systems, Co-authoring and Argumentation Systems, Message Systems and Autonomous Agents which support group collaboration currently exist; however, Department of Defense (DoD) computer security requirements as they impact CSCW systems design has received little attention. This thesis describes CSCW systems and relates group dynamic issues to predict the form of the sophisticated CSCW which will probably become commonplace in the future. Next the Trusted Computer Security Evaluation Criteria (TCSEC) with which all DoD systems must comply are synopsized. An extension of the Bell-LaPadula model underlying the TCSEC requirements is proposed which would allow "Functionally Trusted CSCW" (FT-CSCW), CSCW which would meet many but not all of the TCSEC requirements. Possible first order (efficiency) effects of FT-CSCW, including the effect of sparse group domains, the breakdown of compartmentation, and organizational stratification are discussed. Second order (social) effects are also discussed, as are possible FT-CSCW problems (unstable group membership, attempts to implement Quality Improvement Circles, inter-group CSCW and the effect of visitors.) Finally, some suggestions are made for future FT-CSCW research.

iii

TABLE OF CONTENTS

v

LIST OF FIGURES

I. INTRODUCTION

In this thesis the author examines the security aspects of Computer Supported Collaborative Work (CSCW) and Groupware, its enabling software. CSCW has been described by some as computer-based tools which can be used to facilitate the exchange and sharing of information by work groups. Others have described it as a computer-based shared environment that supports two or more users. [Bock92]

CSCW is a rapidly developing field that has attracted the attention of a growing number of academics and commercial vendors. Computer scientists are devising algorithms to support concurrent activity; human factors specialists are tackling the formidable challenges of group interfaces; telecommunications firms are already looking for ways to exploit the growing demand for collaborative products; and behavioral and social scientists are trying to develop an understanding of how work groups and cooperative technologies will impact on the workplace. [Grud91]

Concurrently, computer security is also an active field of ongoing academic and commercial development. Government computer systems are required to address security concerns by legal mandate, but non-governmental organizations also recognize the value of protecting the secrecy, integrity, and availability of their systems [Ricc93]. In response to the demands of the marketplace, Apple, IBM, and Microsoft are integrating significant security features directly into their

1

next generations of operating systems software [Schn92] [Ricc93]. Some researchers are considering extensive operating systems reengineering in order to support trusted application programs [Grau92]. Others are concerning themselves with social issues, such as the legal implications of E-Mail privacy [Axsm92].

Some authors have raised the issue of security with respect to CSCW [Mars92] [Pres92] and distributed systems in general [Ryme92], but in the author's opinion, to date the discussion has been poorly focused and somewhat cursory. Part of the problem is that different authors often mean very different things when they discuss computer security. *Secrecy*, *data integrity*, and *system availability/reliability* together comprise *computer security* [Pfle89], but the security discussion with respect to CSCW has emphasized technical issues which most directly impact collaboration on networks and resource-sharing. The data integrity and system availability/reliability aspects of the security problem have received the lion's share of attention, while the secrecy aspect of the problem has received little attention. Dennis Eskow has written an excellent article which relates information secrecy issues to civilian computing [Esko93]; however, his article is very much the exception.

The author sees a danger of standards and protocols being developed which optimize collaboration, resource sharing, and "open" CSCW, but which either fail to address the *secrecy* aspect of the security equation in any meaningful way, or worse, make the protection and control of user

2

organizations' information assets *even more difficult* than it is today. Military organizations are *required* to address the secrecy problem. Unless the Secrecy aspect is addressed by the academic and commercial communities, military organizations will be able to use CSCW products only under conditions compatible with the lowest levels of security control. The expected advances and advantages of CSCW will bypass the most important military Information Systems unless and until the secrecy aspect of the computer security problem is addressed. The author realizes that many of the issues and concerns involved may seem esoteric to civilian readers; in fact, making the issues and concerns *less* esoteric is the principle motivation behind this thesis.

In this thesis the author will address several questions: Can sophisticated CSCW be accomplished on a trusted system, and if so, how will security constraints affect organizational structures and the accomplishment of group work?

Chapter II presents a brief discussion of CSCW and groupware with the goal of determining the applications and features which will probably characterize the sophisticated CSCW of the future.

Chapter III addresses the current federal computer security requirements as delineated by the National Computer Security Center's (NCSC) Trusted Computer Security Evaluation Criteria (TCSEC), the "Orange Book." Meeting the TCSEC requirements is a legal mandate for all government systems and software procurement actions, and any government

3

organization which recognizes the value of CSCW and wishes to apply cooperative computer technology to the accomplishment of their mission will *have* to deal with the Orange Book restrictions. Chapter III will also discuss some of the recognized problems with the TCSEC requirements, and will introduce the draft Federal Criteria which may replace the Orange Book.

Chapter IV describes a high level conceptual scheme by which functionally trusted CSCW might be accomplished, CSCW which meets many, but not all, of the Orange Book requirements. The scheme requires extensions to the underlying principles of the current Orange Book requirements in order to work, and the chapter will broadly describe the extensions required. ᵃext, a hypothetical user interface will be described in c ᵤer to illustrate how work would be accomplished in a funct. ᵢnally trusted CSCW environment.

Chapter V describes some of the first-level (efficiency) and second-level (social) effects that might be experienced by organizations attempting functionally trusted CSCW. Special attention is paid to internal organizational structure, information compartmentation, and inter-organizational effects.

Chapter VI provides a summary of this thesis and makes recommendations for future research.

II.   CSCW

Mark Weiser and his colleagues at the Xerox Palo Alto Research Center use the terms "ubiquitous computing" or "embodied virtuality" to describe the computing environment of the future. In this environment, computing technology would be an integral, invisible part of peoples's lives, as pervasive and omnipresent as writing on paper is today. Information would be freely transported and manipulated, and the underlying technology would be widely distributed, embedded in the everyday world. Current concepts like Workstation, Local Area Net (LAN), and Wide Area Net (WAN) would be obsolete, replaced by a generalized information realm permeating virtually all human activity.   No spectacular breakthroughs in hardware or software development are required to make this vision a reality. Evolutionary improvement in display devices and wireless network technologies will provide the prerequisite hardware, and evolutionary improvement in scheduling, meeting, messaging, and conferencing applications, as well as standards allowing open information exchange, will provide the prerequisite software. [Weis91]

Although Weiser never uses the terms CSCW or Groupware in his article, it is clear to this author that the system of applications and software functionality that makes Weiser's vision of ubiquitous computing possible are the descendants of today's Groupware. This thesis is concerned with the

5

security aspects of CSCW, but the current state of groupware is of less interest than the direction in which academic and commercial inquiry is taking us. Let us begin to understand that direction with an examination of the range of functionality described by the term Groupware that will allow sophisticated CSCW to emerge.

A. OVERVIEW OF CSCW CLASSIFICATION SYSTEMS

Classification is usually the first step towards understanding; however, one's choice of criteria can act as a filter, highlighting some properties while obscuring others. Fortunately, nothing prevents us from using more than one set of criteria. Rodden and Blair examine existing cooperative systems using four different modes of classification: **system tasks, form of cooperation, geographic distribution,** and **style of control** [Rodd92]. Their discussion is comprehensive, and in the author's opinion, provides an excellent framework for an understanding of CSCW. As will be seen, Rodden and Blair's modes of classification address almost all of the relevant issues germane to developing a general understanding of CSCW and Groupware. Other authors use taxonomies which address the same issues from slightly different perspectives, and some of these systems will also be discussed in this section.

1. System Tasks

Rodden and Blair first classify Groupware applications according to the type of work they are designed

to accomplish. Based on this first criteria, they recognize four general classes of cooperative systems:

a. *Message Systems*

As networks designed to support communication become more widespread, electronic mail (E-mail) applications increase in complexity and functionality. Each of the currently available message systems make use of proprietary message formats.[Rodd92] Under the taxonomy of Sproull and Kiesler, such systems are called "Type 4 Groupware."[Spro91] Examples of such systems include *COSMOS, AMIGO, Object Lens, Strudel, ISM* [Rodd92], *Microsoft Mail, Lotus cc:Mail* [Higg92], and Wang Laboratories' *FreeStyle* multimedia communication system [Fran91].

b. *Computer Conferencing*

Also derived from E-mail systems, conferencing systems group messages, usually by topic. More recently, reliable high-speed conferencing systems which allow members to communicate in real time have emerged (e.g. *RTCAL,*) and the latest developments are desktop conferencing systems which merge real-time conferencing with a shared windows environment. [Rodd92] Under the taxonomy of Sproull and Kiesler, such systems are called "Type 2 Groupware." [Spro91] A further development is multimedia conferencing systems which integrate text, audio, and full-motion video (e.g. *Rapport, MERMAID* [Rodd92], and *GTCS* [Rudy92].)

c. *Meeting Rooms*

Automated face-to-face meeting rooms generally consist of a conference room with a large screen projector, a

7

computer or network of computers, individual input/voting terminals, and a control terminal. The system supporting the meeting often uses multi-user software based on some form of analytical decision techniques, graphics software, and vote tally and display software.[Rodd92] Under the taxonomy of Sproull and Kiesler, such systems are termed "Type 1 Groupware."[Spro91] Examples include *CoLab, Project Nick*, and the University of Arizona's *Planning Laboratory*. [Rodd92]

d. *Co-Authoring and Argumentation Systems*

Such systems support and represent the negotiation and argumentation processes involved in group work. The cooperative authoring of documents, where the final product is the product of a software mediated process of negotiation between the authors, is a current example of this class of system. Examples of argumentation systems include *gIBIS* and *SIBYL*; of co-authoring systems, *Quilt* and *CoAuthor*. [Rodd92]

2. **Forms of Cooperation**

Rodden and Blair also classify CSCW by the way in which group members interact, regardless of the tasks involved.

a. *Purely Synchronous Systems*

Purely synchronous systems require the simultaneous presence of all group members. Typical examples include real-time conferencing systems, and the brain-storming tools sometimes used in meeting room systems. [Rodd92] Sproull and Kiesler call purely synchronous systems "Type 1" or "Type 2" Groupware. [Spro91]

8

b. Purely Asynchronous Systems

Purely asynchronous systems facilitate cooperation *without* requiring the simultaneous presence of all group members. Such systems are often used to tackle structured, prescriptive tasks accomplished through cooperation over an extended time-scale. A typical example is cooperative message systems, where users take on independent roles which produce and consume messages. [Rodd92] Sproull and Kiesler call purely asynchronous systems "Type 4 Groupware." [Spro91]

c. Mixed Systems

Mixed systems allow real-time synchronous cooperation within the same framework as time-independent asynchronous work, and contain elements of both synchronous and asynchronous cooperation. Typical examples would be computer conferencing and co-authoring/argumentation systems. [Rodd92] Other examples of mixed systems are TWS [Ishi91], EuroPARC *Media Spaces* [Caru91], *QED Office-The Administrator* [Dunc92], and the current market leader, *Lotus Notes* [Cast92, Carr92, Cast92, Rayl92, Sull92].

3. Geographic Distributions

Rodden and Blair's third system of classification involves the distribution of the users of the system. (Under this system the dichotomy between remote and co-located systems is as much a *logical* concept as a *physical* relationship. It is concerned with the accessibility between users rather than their physical proximity.)

9

a. Co-located Systems

Purely co-located systems require the local presence of all group members. Purpose built meeting rooms with a large projected screen linked to a LAN of desktop computers provide a typical example. [Rodd92]

b. Virtually Co-located Systems

Similar to purely co-located systems, virtually co-located systems do not require all users to be in one room to function. Real-time multimedia conferencing systems such as *MMConf* and *Cruiser* provide typical examples. [Rodd92]

c. Locally Remote Systems

Locally remote systems provide high-bandwidth real-time accessibility between users, often using shared screen techniques. Co-authoring and argumentation systems (*Quilt* and *gIBIS*) and real-time conferencing systems (*RTCAL*) provide typical examples. [Rodd92]

d. Remote Systems

Remote systems assume the existence of only minimal accessibility between users. message systems which assume only simple communication systems and computer conferencing systems which assume only rudimentary 'dial-in' connectivity provide typical examples. [Rodd92]

The interrelationships of the first three classification modes are depicted in figure 1.
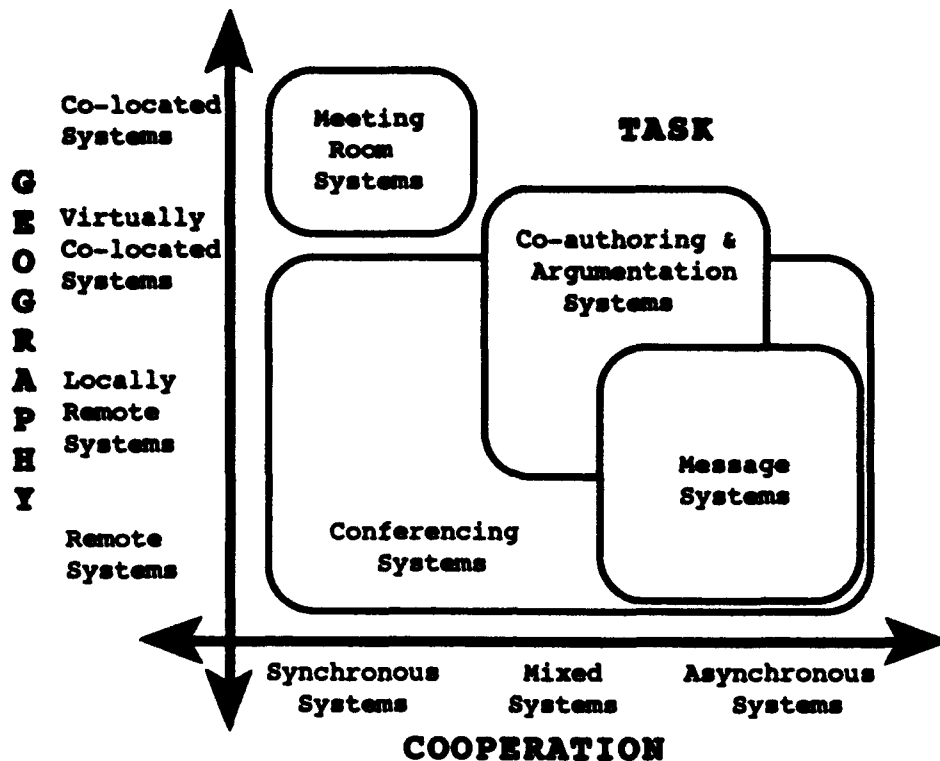
Figure 1. Interrelationships of System Task, Form of Cooperation, and Geographic Methods of CSCW Classification.

4. Styles of Control

In the author's opinion, Rodden and Blair's fourth classification system, which is based on the style of control a Groupware application supports, presents a valuable point of departure for those most interested in the psychological or management science aspects of CSCW, while at the same time providing a means of relating existing or conceptual CSCW systems to technically similar distributed systems.

Rodden and Blair recognize five different control styles which range along an axis with *unstructured tasks* at one end

and *prescriptive tasks* at the other. Unstructured tasks are those requiring creative input from a number of users and which are not often able to be detailed or described in advance (for example, software design.) Structured tasks are those involving existing solutions and procedural cooperative mechanisms (for example, invoicing procedures used in large organizations.) [Rodd92]

a. *Speech Act or Conversation Based Systems*

Such systems apply a linguistic approach based on speech act theory. Cooperation is represented and controlled using some form of network structure which details the patterns of messages exchanged. Examples of such systems are *Coordinator* and *CHAOS*. [Rodd92]

b. *Office Procedure Systems*

This class is characterized by the use of some form of procedural language to describe and control group cooperation by defining roles and activities. Tasks performed are described in terms of the effect of concombinant sub-tasks or procedures. Examples of such systems include *POLYMER, AMIGO,* and *COSMOS*. [Rodd92]

c. *Semi-formal, Active Message Systems*

Semi-formal systems automate the most amenable tasks while allowing other parts of the system to remain manual. Examples are the *Object Lens, Strudel Project,* and *ISM* systems. [Rodd92]

d. *Conferencing Systems*

Conferencing system control mechanisms are generally minimal and fixed to applications. Traditional conferencing

systems have human conference mediators while in more modern real-time systems, most of the control is embedded in the conferencinq application software. [Rodd92]

e. Peer-group Meeting or Control Free Systems

This class of systems imposes little or no control on users. Group members are allowed to formulate their own protocols, and generally all users have equal status and may amend and use the system freely. An example is the CoLab system. [Rodd92]

Systems which exemplify the first three control styles exhibit *explicit* control while the last two exhibit *implicit* control. Rodden and Blair use this observation to relate CSCW control styles to distributed systems technical issues (see below.) [Rodd92]

5. Autonomous Agents

There is one emerging aspect of Groupware which Rodden and Blair do not address: autonomous agents. Such agents are "independent" software routines which support the user, represent the user to the system, and handle complex interactions with other cooperative agents and system resources [Lee93]. Autonomous agents may be designed to be highly visible and interactive, mimicking human assistants or team members (Intelligent Agents); or they may be designed to act "behind the scenes," invisible to the user (Coordination Systems).

a. Intelligent Agents

An intelligent agent is a virtual participant in a

group process. For example, an electronic game system might generate a non-human player automatically or at the human players' request. Intelligent agents may be designed to fill roles similar or different from the human participants. [Elli91] They are similar to Bock's Active Information Agents [Bock92].

b. Coordination Systems

Often called the Links and Active Coordinators [Bock92], Coordination Systems relate individual and group actions to goals. [Elli91] They can be categorized by their underlying control models (which in turn are similar to Rodden and Blair's styles of control.) Typical coordination systems include:

- Form or document routing models.
- Procedure or process programming models.
- Conversation oriented models.
- Communication or role relationship models. [Elli91]

6. The Basic Questions of CSCW Classification

As was noted above, several similar Groupware taxonomies are in the literature; however, the author has observed that in general all of the systems are concerned with the same basic questions:

- What is the group task?
- What form of cooperation is required?
- What are the relative locations of the participants?
- What form of control is in operation?

The answers to these questions classify any given CSCW system, but another aspect of CSCW is relevant to our understanding of Groupware—the social aspect.

B. THE SOCIAL ASPECTS OF CSCW

> A couple of years ago, a designer working on an executive support system candidly observed that "If you automate a mess, you are going to get an automated mess." No longer are we simply applying technology to expedite standard operating procedures. Rather, we are concerned with altering operations and policies so that business teams can "work smarter." [Bock92]

Sproull and Kiesler observe that while technological systems are usually designed and implemented by organizations in order to achieve predictable first-level efficiency effects, almost inevitably the system chosen leads to unexpected second-level social effects [Spro91]. A logical task for social scientists is to predict these second-level effects, and use their knowledge of these effects to influence CSCW systems design. Among the authors who embrace this role is Rob Kling, who goes so far as to state that "the social dynamics of work make CSCW a social movement rather than merely a technological advance." [Klin91] Group dynamics is a useful perspective from which to approach the most relevant social issues. A brief examination of the basic principles involved will provide the basis for a discussion of the social aspects of sophisticated CSCW at the conclusion of this chapter.

1. Group Dynamics

Cole and Nast-Cole provide an excellent primer of group dynamics and how the issues raised relate to CSCW design. They note that human group behavior occurs at three simultaneous levels: the *individual*, the *interpersonal* (dyadic), and the *group*. It is important for an observer of any group to be conscious of the behavioral level under study. One's choice of level will act as both a lens and a filter; it will simultaneously focus and obscure the phenomenon under study. They further observe that we have a tendency to observe and attempt to explain group behavior at the individual level, even when this is probably inappropriate. Just as different perspectives are useful for understanding (and classifying) CSCW systems, different perspectives are useful for understanding group behavior. [Cole92]

a. Purpose and Communication

New groups spend time establishing a group purpose, a set of common goals. The group members then align their personal (private) goals with the group's goals, after which, the group pursues their common purpose through communication at the group level. Simple communication is the exchange of information between individuals; however, *group* communication occurs only if the individuals *assign a common meaning* to the information. [Cole92]

b. Content and Process

Content refers to the information being exchanged or the analysis in progress. It is the *actual work* in which the

16

group is engaged. Process is the *means* by which the group accomplishes its work, that is, the methods and procedures the group employs. Content and process must be observed simultaneously, for only together do they provide the full context of group actions. [Cole92]

c. *Task and Maintenance Activities*

Task activities are those activities which can most directly be traced to the group purpose, while maintenance activities are those which reinforce the structure and function of the group. For example, a group meeting might spend the minority of its time discussing recognized agenda (task) items and the majority of its time on seemingly irrelevant social discussions which in fact are reinforcing group communication and aligning individual and group goals (maintenance). [Cole92]

d. *Roles*

Roles are stances from which individual group members operate for a limited period of time, and which are not directly related to job titles. Different roles, such as "mover, opposer, follower, and bystander" are generally recognized by the group, and a variety of social clues (also recognized by the group) signal a role change. For example, a group member might use *passive* body language to signal the adoption of the role of *bystander* in order not to interfere in a heated group debate, then later use *active* body language to signal the adoption of the role of *mover* or *opposer* in order to help resolve the conflict. [Cole92]

17

e. *Norms*

Norms are the commonly shared beliefs, attitudes, and viewpoints that operate as a set of standards for the group. Norms set the bounds of acceptable and unacceptable group behavior. A specific set of group norms develop and evolve over time, and are especially influenced by the behavior of high-status group members. [Cole92]

f. *Leadership*

Good leadership is the great intangible of group dynamics. Leaders must be concerned with group purpose and communication. They must insure that content and processes balance task and group maintenance activities, and through the use of roles and norms leaders can exercise a profound influence on group efficiency and effectiveness. [Cole92]

2. Stages of Group Development

Cole and Nast-Cole subscribe to Tuckman's five serial stages of group development. These stages are predictable steps in the maturation process of any group. The rate and quality of the group's maturation is determined by the quality of the group's experience at each successive stage. These stages are:

- **Forming** – the social process of inclusion and orientation.
- **Storming** – the process of testing bounds, processes, and capabilities.
- **Norming** – a fine-tuning of group relationships; the building of team spirit.

18

- **Performing** – the highly-productive stage of a mature group.
- **Adjourning** – wrapping-up after work is complete; the process of closure. [Cole92]

Even an *ad hoc* group thrown together to handle a crisis situation will pass through these stages—however briefly or imperfectly. Even a group interrupted in its task will pass through the remaining stages before it dissolves. Anyone concerned with group dynamics (or the design of systems which support group dynamics) will find it useful to be able to recognize these stages and support their group dynamic functions. [Cole92]

3. Group Dynamics and CSCW

Group dynamic theory suggests that any component of a group system needs to be understood in the context of the whole. Cole and Nast-Cole observe that this is also true for the computer technology component of a system. The group leader's commitment (or lack thereof) can determine whether or not CSCW will gain acceptance. A system which does not have provisions which allow group members to be aware of other participants' transitory roles and normative states will make an ineffective conference or co-authoring system. Further, a system which does not recognize the maintenance activity requirements of a group and supports only the task activities will find the group members going off-line to conduct required social interchange. Lack of immediate feedback and traditional social cues in a poorly designed

19

user interface may cause social dysfunction in a group attempting to accomplish politically challenging work. [Cole92]

There are other social dynamic problems which plague CSCW. Kyng notes that currently while manual work is often accomplished through cooperative means, computer work is not. This is largely a historical artifact which to a large extent will be self-correcting as collaborative IS technology matures. [Kyng91] The situation is ironic, because not only has collaborative technology begun to mature, it has begun to outstrip prevailing management attitudes. One barrier to telecommuting is the perception that geographically remote workers will be "invisible" and unable to be effectively managed or controlled. Groupware has already improved to the point that this perception is largely unfounded. [Peri91]

CSCW systems can exhibit a variety of control styles in *order to accomplish a variety of tasks in a variety of social* contexts. For this reason, no single prescriptive set of CSCW requirements is possible; however, Rodden and Blair make the following observations concerning group dynamics and groupware design. [Rodd92]

- The organizational context of the work needs to be captured.
- The many different forms of cooperation need to co-exist.
- The structure and organization of groups need to be explicitly recognized.
- Groups work in dynamic and unexpected ways.

- Groups are themselves dynamic.
- Control should be enabling rather than constraining.

In the author's opinion, all of these observations are valid. Group dynamic principles must form the conceptual framework for Groupware design. Technical considerations must give way to social considerations. Groups cannot be expected to accommodate their work habits to CSCW systems which do not support the group's social needs.

C. CSCW ON DISTRIBUTED SYSTEMS

Rodden and Blair observe that in most distributed systems the problem of shared access is handled by masking out the existence of other users. Until recently the emphasis has been on non-cooperative tasks, because it was thought to be important to "protect" users from the underlying details of the computing environment. This "distribution transparency," the conscious design of systems which mask all of the problems inherent in distributed systems, clearly contradicts the requirements of CSCW. Distributed system complications (and solutions), such as location (naming servers), access (remote procedure call protocols), migration (load balancing strategies), replication (multiple copy upgrade algorithms), and concurrency and failure (distributed atomic transaction mechanisms), have all been approached as problems requiring prescriptive resolutions. Unfortunately, labile, complex activities such as CSCW are *constrained* by prescriptive solutions as often as they are empowered. In certain CSCW

situations, a groupware application needs to "know" many of the things that are being masked by the distributed control system. In this light, a fresh approach to distributed systems control is needed in order to support sophisticated CSCW with any degree of efficiency. [Rodd92]

1. CSCW Tailored Distributed System Control

Rodden and Blair acknowledge that little work has been done in the area of distributed systems control tailored to the needs of CSCW; however, they identify three possible lines of approach:

a. Clean separation of mechanisms and policies

If there is a clean separation between distribution management control mechanisms and the policies which control the use of those mechanisms, CSCW application programmers would be free to turn on and off mechanisms which might otherwise obstruct CSCW. [Rodd92]

b. Tailored mechanisms

A single set of mechanisms is unlikely to be suitable for any given CSCW application, therefore, development of a collection of mechanisms tailored to specific applications is one possible approach. This approach might best be suited to CSCW activities best suited for implicit styles of control, such as speech act and conversation based systems, office procedure systems, semi-formal systems, and active message systems. [Rodd92]

c. Tailored policies

Distribution policies provide the avenue of approach

22

to CSCW best suited to explicit control mechanisms, such as conferencing systems, peer-group meeting systems, or control free systems. They stress that "it is important to avoid these policies overly inhibiting the cooperation of users." [Rodd92]

In the author's opinion, Rodden and Blair's discussion is particularly instructive. Standards and policies which were designed to support one style of computing may be inappropriate and constraining with respect to another style. Their desire to accommodate distributed systems control to the needs of CSCW is laudable, but what of the need for security? If standards which support a stand-alone style of computing are to be replaced by standards which support a cooperative style of computing, shouldn't we insure that these new standards support the secrecy, data integrity, and system access needs of all users?

D.   THE FUTURE OF GROUPWARE

Before addressing security concerns directly, the features and functionality which will characterize the groupware of the future must be stated explicitly. In the authors opinion, the sophisticated CSCW of the future will be made possible by Groupware and underlying computing technology which will provide the following functionality.

1.   Tasks, Cooperation, and Geography

Sophisticated Groupware will support all forms of communication between group members. Message exchange,

conferencing, co-authoring, and argumentation will be supported, regardless of the geographic dispersion of group members. Every form of cooperation between group members, synchronous and asynchronous, will be supported, both separately and simultaneously.

2. Styles of Control

Sophisticated Groupware will be characterized by a variety of styles of control, each appropriate to the task at hand. Groups will be engaged in a variety of specific tasks, some structured, and some unstructured; therefore, no single style of control will be appropriate for all uses.

3. Group Dynamic Support

Sophisticated Groupware will only be possible in an environment which supports individual and group communication needs. Both task and group maintenance activities will be supported, as will role-playing, norm formation, and the transmission of any information needed for the group members to be kept aware of group developmental stage transitions as they pass.

4. The User Interface

The user interface of sophisticated Groupware will be characterized by a curious paradox. Where needed, the interfaces will be rich in group dynamic cues, enabling group members to navigate from task to task while at the same time being able to maintain awareness of the changing social

fabric. At the same time, in the ubiquitous computing environment of the future [Weis91], many group dynamic cues will be provided by the fully integrated context of group activities. In other words, when knowledge of the computing context is required to accomplish work (e.g. asynchronous message exchange) the interface will be specifically designed to provide group dynamic information, but when knowledge of the computing context is *not* required (e.g. full-motion video conferencing) the transparency of the interface will allow exchange of group dynamic information without any special provisions.

5. Links, Coordinators, and Agents

A further characteristic of the sophisticated CSCW of the future will be that many of the prescriptive, rule-based tasks and activities which presently occupy our time and limit the efficiency of groups will be handled by non-human assistants. Whether called intelligent agents [Elli91] or active information agents [Bock92] these assistants will be a common feature of the ubiquitous computing environment.

E. CONCLUSION

It is evident that the sophisticated Groupware to come will support open communication within working groups, will be rich in social information and group dynamic cues, and will have automated routines accomplishing prescriptive work at the individual, interpersonal, and group level; however, such a system presents significant challenges with respect to

security. Free access to all information in the group domain may facilitate CSCW, but some information must always be protected. Even for organizations not overly concerned with secrecy, data integrity and system availability will be desired; however, Department of Defense (DoD) organizations are concerned with secrecy, both for reasons of military necessity and by legal mandate. The next chapter will discuss the security requirements with which DoD organizations (and all government agencies) must contend.

III.   COMPUTER SECURITY REQUIREMENTS

This chapter will examine the current federal computer security requirements, as well as what in the author's opinion is the principle sticking-point preventing the total alignment of the DoD's information security (INFOSEC) requirements with the DoD computer security requirements: the "Human Trust Problem."

As was briefly discussed in Chapter I, the current requirements have been promulgated by the National Computer Security Center (NCSC) in the "Rainbow Series," the lead publication of which is the "Orange Book." An examination of the terms, requirements, and rationale embodied in the Orange Book is more than an exercise of interest to federal bureaucrats and military personnel. As *major customers of commercial systems*, U.S. Government agencies are in a position to profoundly influence the development and evolution of technical standards. Thus even organizations not governed by federal security requirements may find the requirements impacting the available choice of products. [Ricc93]

The Orange Book is 121 pages in length, and the entire Rainbow Series is a total of 1,678 pages. It is not the intention of this chapter to discuss all aspects of the Rainbow Series in full detail, but rather to summarize the embodied requirements as the basis for a later discussion of trusted CSCW. The following is derived directly from the

Orange Book [OrBk85]; however, other authors provide similar summaries, with differing emphases [Chok92] [Ricc93].

A. THE MILITARY SECURITY MODEL

The hierarchical classification scheme used by the DoD to describe the level of protection which is afforded important information and processes is commonly referred to as the military security model. The model is a lattice which incorporates both mandatory and discretionary control. Control is accomplished by a system of background investigations which afford an individual *potential* access to objects at a given classification level (mandatory control). Once potential access to a given level is granted, an individual will be given *actual* access to specific objects based on the requirements of their current responsibilities, on their "need-to-know" (discretionary control.)

In increasing order of sensitivity, the military model hierarchical classification levels are: *Unclassified*, *Confidential*, *Secret*, and *Top Secret*. Information or processes may also be placed in *compartments*; that is, they may be placed in categories based on their subject or utility. Compartments are often used as a convenient means to administer discretionary control. A hypothetical object might be classified *secret, NATO*. It is held (protected) at the *Secret* level, and is in the *NATO* compartment. Classification level and compartment, together, comprise an object's full classification. [OrBk85] Numerous DoD policy

statements mandate both mandatory and discretionary security controls. [OrBk85, pp.74-76]

Non-governmental organizations might rename the levels of classification (*public*, *sensitive*, *proprietary*), and they will certainly create their own compartments (*sales*, *project-blue*, *quality-work-group*), but many private firms have adopted the most important elements of the military model for their own purposes; however, the fact that the government's mandatory control classifications have legal standing creates an important distinction between non-governmental and governmental (especially DoD) organizations. Private organizations can *decide* to infer controls equivalent to mandatory access controls, based on cost analysis or any other paradigm. Governmental organizations have *no such freedom*. *Secret* material is *Secret* material, and must be treated as such until its status is changed by the appropriate authority. [Ricc93]

B.   ORANGE BOOK CRITERIA

The evaluation criteria defined in the Orange Book apply to commercially available automatic data processing systems (ADP), to the specification of security requirements for ADP systems acquisition, and to the evaluation of existing systems. In general, the criteria provides a basis for evaluation of the effectiveness of technical security controls built into ADP systems, the means by which a system may be declared to be reasonably "secure." The criteria specify that a trusted system will control, through the use

29

of specific security features, access to information such that only *properly authorized individuals, or processes operating on their behalf*, will have access to or the ability to read, write, create, or delete information. [OrBk85, p.3]

1.   Fundamental Computer Security Requirements

There are six fundamental Orange Book requirements, the implementation of which infer a level of trust upon a system. The first two requirements deal with the general category of *policy*, the third and fourth with the general category of *accountability*, and the fifth and sixth with the general category of *assurance*.

a.   Requirement 1 — SECURITY POLICY

"There must be an explicit and well-defined security policy enforced by the system." A set of rules must be used by the system to determine whether a given subject can be permitted to gain access to a specific object. Both mandatory and discretionary access controls are required. [OrBk85, p.3]

b.   Requirement 2 — MARKING

"Access control labels must be associated with objects." The system must mark every object with a label that reliably identifies the object's classification level, and/or the modes of access accorded those subjects who may potentially access the object. [OrBk85, p.3]

c.   Requirement 3 — IDENTIFICATION

"Individual subjects must be identified." Information access must be mediated on the basis of the identity and

30

authority of the individuals attempting access. Identification and authorization information must be "securely maintained" by the system and must be associated with every active element that performs security-relevant actions in the system. [OrBk85, p.4]

d. *Requirement 4 — ACCOUNTABILITY*

"Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party." The system must have an audit log which records the occurrence of security-relevant events; however, the necessity of a capability to select audit events in order to minimize the expense of auditing and to allow efficient analysis is recognized. Audit data must be protected from unauthorized modification or deletion in order to permit post-violation investigations. [OrBk85, p.4]

e. *Requirement 5 — ASSURANCE*

"The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above." There must be an identified and unified collection of hardware/software controls which perform the functions of security policy, marking, identification, and accountability. These controls are "typically embedded in the operating system" which is *designed* to be secure. Sufficient documentation is required to make possible independent evaluation of the compliance (and the basis for the *assertion* of compliance) with the other requirements. [OrBk85, p.4]

f. Requirement 6 — CONTINUOUS PROTECTION

"The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes." This requirement applies throughout the system's life cycle. [OrBk85, p.4]

The requirements form the basis for the *Orange Book criteria classes*, the classification scheme used to describe a system's level of compliance.

2. Orange Book Criteria Classes

The classes are hierarchical and are divided into four divisions, some of which are further subdivided. They are: D, C1, C2, B1, B2, B3, and A1, with class A1 being the highest. The criteria are transitive; that is, achievement of a given level implies compliance with *all* requirements of *all* lower levels. Four major criteria are addressed in order to determine a system's class: security policy, accountability, assurance (the fundamental requirements), and documentation (the written user guides, manuals, and test/design documents required for each division.) Relevant to any understanding of the criteria is an understanding of the concept of a *Trusted Computing Base* (TCB). The TCB is the totality of all protection mechanisms within a system, hardware, firmware, and software. It is all of the features which are responsible for the enforcement of a security policy, and no security features relevant to the Orange Book requirements can be considered to be external to a system's TCB [OrBk85, p.67]. For example, a bulk encryption mechanism

32

used by a long-haul telecommunication network could be considered part of a hypothetical system's TCB only if the hypothetical system had actual control of the telecommunication network. The following summaries give a general idea of the requirements of each class.

a. *Class D: Minimal Protection*

Class D implies that a system has been submitted for evaluation but has failed to achieve a higher classification. In other words, a class D system provides no real security. [OrBk85, p.93]

b. *Class C1: Discretionary Security Protection*

The TCB of the system nominally satisfies discretionary security requirements by separating users and data. Some credible controls capable of enforcing access limitations on an individual basis are incorporated. "The C1 environment is expected to be one of cooperating users processing data at the same level of sensitivity." [OrBk85, p.93]

c. *Class C2: Controlled Access Protection*

The system enforces a more finely grained form of discretionary access control, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and system resource isolation. [OrBk85, p.93]

d. *Class B1: Labeled Security Protection*

The system features an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects. The capability for

accurately labeling exported information must exist. Flaws discovered during testing must be removed. [OrBk85, p.93]

e. *Class B2: Structured Protection*

The TCB is based on a clearly defined and documented formal security policy model that requires discretionary and mandatory access control enforcement to be extended to all subjects and objects in the ADP system. In addition:

- Covert channels are addressed (see section 4 below.)
- The TCB is carefully structured into protection-critical and non-protection-critical elements.
- The TCB interface is well-defined.
- The TCB design and implementation enable more thorough testing and review.
- Authentication mechanisms are strengthened.
- Support for system administrator and operator functions provide trusted facility management.
- Stringent configuration management controls are imposed.
- The system is "relatively resistant" to penetration.

[OrBk85, p.94]

f. *Class B3: Security Domains*

The TCB must satisfy reference monitor requirements (see section 4 below.) It must mediate all accesses of subjects to objects, be tamperproof, and be sufficiently small to allow analysis and tests. The TCB is structured to exclude code not essential to security policy enforcement with significant engineering effort during design and implementation directed towards minimizing complexity. A Security Administrator is supported, audit mechanisms signal

security-relevant events, and there are system recovery procedures. The system is "highly resistant" to penetration. [OrBk85, p.94]

g. *Class A1: Verified Design*

A1 systems are "functionally equivalent" to B3 systems; however, the development and implementation of the system has been so carefully and formally modeled and designed, and so thoroughly tested and documented, that it can be stated that *all* security requirements have been met "with a high degree of assurance." [OrBk85, p.94]

All of these class requirements are discussed in much greater detail in the Orange Book itself, and even further detail and amplification is provided by the remaining volumes of the Rainbow Series.

3. System Operating Modes

Another concept relevant to our discussion is that of system operating mode. A system's operating mode classification describes the clearances of the systems users and the manner in which the system processes sensitive information. (The following definitions are from the instruction which implements the Department of the Navy Automated Information System Security Program [NAISSP], and as such impart formal significance to a system's configuration description; however, the author will use these terms in subsequent chapters in a less formal manner. That is, if the author refers to a hypothetical system as operating in one of the following modes, this will not imply

full compliance with Department of the Navy requirements, but simply to the clearances granted to the systems' users.)

a. *Dedicated Security Mode*

All system users possess the proper mandatory and discretionary clearance for accessing all data processed and stored in the system. All information in the system is handled at the highest level processed; that is, if the highest level processed by a given system is *Top Secret*, and the system is operating in dedicated security mode, then all information in the system is treated as if it were *Top Secret*. [NAISSP]

b. *System High Security Mode*

All system users have the mandatory clearance for accessing all data; however, *not* all users have the same discretionary clearance, the same "need-to-know." As in Dedicated Security Mode, all information in the system is handled at the highest level processed. [NAISSP]

c. *Multilevel Security Mode*

Some users using the system do not have the required (mandatory) clearance for accessing the most sensitive classified data processed and stored by the system. Trusted data labels are maintained by the system. [NAISSP]

4. Other Orange Book Terms and Concepts

There are other security related terms and concepts discussed by the Rainbow Series which will become relevant to our discussion of the security aspects of CSCW. These include:

a. *The Bell-LaPadula Model*

The Bell-LaPadula model is a formal state transition model that describes a set of access control rules. The model divides all entities in a system into *subjects* (active entities that cause information flow) and *objects* (passive entities that contain or receive information), and enforces a "secure state" by use of two properties:

● The Simple Security Property — An subject may only read objects of the same or lower sensitivity level than itself.

● The ★-Property — A subject may not write to objects of a lower sensitivity level than itself. [Pfle89]

The Bell-LaPadula forms the basis and formal conceptual rationale for the Orange Book requirements [JaBk92, pp.6-7].

b. *Covert Channel*

A covert channel is a communication channel that allows a process to transfer information in a manner that violates the system's formal security policy. Covert channels may involve *storage* (the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process) or *timing* (in which one process signals information to another by modulating its use of system resources in such a way as to affect the real response time observed by the receiving process.) [OrBk85, p.112]

c. *Front-End Security Filter*

A front-end security filter is a routine that is invoked in order to process data as required by the system's security policy prior to the data being released outside the

TCB or immediately upon receiving data from an external source. [OrBk85, p.113]

d. *Reference Monitor Concept*

A reference monitor is an abstract machine that mediates all accesses by subjects to objects. [OrBk85, p.115]

e. *Security Kernel*

The security kernel of a system is all the hardware, firmware, and software elements of a TCB that implement the reference monitor concept. It must mediate *all* accesses, must be protected from modification, and must be verifiable as being correct. [OrBk85, p.115]

f. *Security Relevant Event*

A security relevant event is *any* event that attempts to change the security state of the system, and *any* event that attempts to violate the security policy of the system. (Hence, both *authorized* and *unauthorized* change attempts are security relevant events.) [OrBk85, p.115]

g. *Sensitivity Label*

A sensitivity label is an information unit that represents the security classification of an object. The TCB uses sensitivity labels as the *basis for* mandatory access control decisions. [OrBk85, p.115]

5. The Human Trust Problem

The DoD information security systems have always relied on the element of trust, in the form of self-censorship, to allow humans cleared to access high level information to interact with humans only cleared for low

level information. Hence Commanding Officers, possessing the highest levels of clearance at their commands, may converse and correspond with any and all members of their commands, and they are *trusted* not to divulge unauthorized information [INFOSEC]. This state of affairs may occasionally lead to the leaking of information, but in the author's opinion, security minded organizations have little choice but to rely on the discretion of their members.

The human users of any computer are as much a part of the system as the hardware, firmware, or software. The Orange Book recognizes human users as system elements; however, its reliance on the Bell-LaPadula model leads to direct complications. Technology cannot be *granted* trust based on a background investigation. Technology must be *empirically proven* to be trustworthy. Mechanical systems which comply with the restrictions of the Bell-LaPadula model *can* be proven trustworthy [Pfle89], but since it cannot be guaranteed that the human elements of an information system would *never* violate the ★-property (i.e., that high-level individuals would *never* interact with low-level individuals), full system trust certification of a multi-level system is somewhat problematical [OrBk85] [Ricc93]. This "human trust" dilemma has lead to the call for revised computer security standards, which are briefly discussed below.

6.   CSCW and the Orange Book

Ignoring for the moment the consequences of the human trust problem, the concepts and requirements of the

Orange Book lead to several constraints which in the author's opinion would characterize any "trusted" computer system capable of supporting sophisticated CSCW.

In the author's opinion, the Orange Book requirements are conceptually oriented towards a view of computer systems as stand-alone systems. Since the preservation of secrecy is the paramount goal, isolation of the TCB (if not the system in its entirety) is seen as the solution to the security problem. This perceived predilection for isolating solutions makes the Orange Book especially poorly suited to the solution of cooperative/collaborative security problems.

The Orange Book adopted the Bell-LaPadula model because it was the leading state transition model that could be mathematically verified as preserving secrecy. Regardless of the system operating mode, a *trusted system* (one which has been verified as fulfilling all of the Orange Book requirements) has a TCB which controls all security relevant events. The system's security kernel mediates *all* accesses by subjects to objects. Even if the trusted system were geographically distributed, all elements of the system would be under the control of *one* TCB. Subjects "foreign" to the system would only be allowed access after they had been "naturalized" by passage through a front-end security filter in accordance with the system's security policy. All subjects and objects in the system (even naturalized foreign subjects and objects) would have tamper-proof sensitivity labels, and for the system to operate with reliability and

efficiency, the system's reference monitor would have to be conceptually coherent and relatively straightforward.

It is the author's belief that under such conditions the casual migration of subjects between work groups under the control of different TCB's is not possible. At the very least, coordination of CSCW between *different* trusted systems would require extensive communication between the Security Administrators of each TCB. The degree of constant coordination required would probably be considered onerous by most groups, and at least in the immediate future, distributed inter-system CSCW will probably only be attempted on systems where the user's access authorities approximate the Dedicated or System High Modes of operation.

Intra-system CSCW, still ignoring the Human Trust problem, in which the group works within and under the control of *one* TCB, is not a technically challenging proposition in the Dedicated or System High Modes of operation; however, intra-system CSCW in the Multilevel Security Mode offers coordination and control challenges similar to those discussed above. In the next chapter the manner in which functionally trusted CSCW (FT-CSCW) on a single system operating in Multilevel Security Mode might be conducted will be explored.

C.   DRAFT FEDERAL CRITERIA

Before leaving our discussion of the computer security requirements, it is worth noting that the restrictive nature of the Orange Book requirements is a recognized problem

41

[Ricc93], and a more flexible set of requirements is under development. In the most general terms, the current draft of the new Federal Criteria recognize that not all federal systems should exclusively emphasize system secrecy. Some federal and many commercial systems should emphasize system integrity. The new criteria mandate the formulation of "protection profiles" as part of the systems development process. The TCB is modularized into distinct functions and processes, and a given protection profile would describe and justify a particular collection of TCB module descriptions. The current Orange Book criteria have the intent of defining the means by which *any* system might be declared to be "trusted" or "secure," regardless of the system's intended use. The draft criteria propose a classification system (CS1-CS4) designed to support profiles built around *either* a well defined secrecy *or* integrity model. Under the draft Federal Criteria, the means are described by which a system might be declared to be "sufficiently trusted," or "secure enough." Under the draft Federal Criteria, a military system processing highly sensitive information would probably operate under a protection profile quite similar to the current Orange Book requirements; however, a non-military system processing non-sensitive information would probably develop a protection profile allowing the use of commercial-off-the-shelf (COTS) software that would be totally unacceptable for military use. [FedC92]

It should be emphasized that the new criteria are in draft form and may evolve significantly before they are

42

adopted; however, in the opinion of the author, it is highly probable that for organizations predominately concerned with secrecy (such as the DoD), the principles and concepts discussed in this chapter will bind "trusted" CSCW for the foreseeable future, whether they are operating under the Orange Book criteria or a Federal Criteria protection profile.

IV.   FUNCTIONALLY TRUSTED CSCW

In this chapter the author will develop a conceptual scheme that describes in broad terms the means by which CSCW might be accomplished on a *functionally trusted* information system, an information system that meets all of the orange book requirements with the exception of the human trust problem. This scheme, "Functionally Trusted CSCW" (FT-CSCW), would allow an organization to conduct CSCW with "reasonable security" (although not with the formal certified trust conveyed by full compliance with the Orange Book criteria.)

The FT-CSCW scheme creates sensitivity labels which provide *group* security domain information to the system's security kernel. This allows the reference model to broker all security relevant events with minimal overhead while conceptually organizing objects and subjects into collections that have a "group identity."

As discussed in Chapter III, the Orange Book cannot grant trust to the human members of an IS. This human trust problem is a severe restriction for any organization wishing to attempt trusted collaborative computing. In strict compliance with the Bell-LaPadula model, an individual with a high sensitivity clearance is not even allowed to acknowledge receipt of e-mail from an individual with a low sensitivity clearance (as this would violate the ★-property.) Obviously, some concessions to reality are necessary or CSCW which accommodates the secrecy aspect of computer security will never be possible. FT-CSCW attempts to fill this role.

First, the extensions to Bell-LaPadula needed to make FT-CSCW possible will be described, then a series of definitions and conventions which would allow the creation of group sensitivity labels will be given. Finally, a hypothetical user interface will be used to illustrate how the individuals of a hypothetical organization would accomplish FT-CSCW. The chapter will conclude with a description of "tactical" FT-CSCW, how work in a hypothetical organization would be accomplished at the group level.

A. BELL-LAPADULA EXTENDED FOR GROUPS

FT-CSCW is facilitated by two extensions of the Bell-LaPadula model: a provision for the formal declassification of objects, and the development of a group sensitivity label.

1. The Formal Declassification of Objects

The Bell-LaPadula model has no provision for the declassification of objects, and this would make it impossible for work accomplished by a work group at a higher level to be shared with lower levels. It is proposed that closely guarded utility subjects that declassify objects be allowed. Information security regulations designed for non-automated systems allow (and specify the control requirements for) the declassification of information. Similar allowances should be made for automated systems. The subjects in question should be high privilege utility routines that could only be invoked directly, and only under highly controlled conditions by human users.

It is probably not possible to formally prove that systems with declassification channels are totally secure, hence this provision is a deviation from the current Orange Book concept of trust. It is a concession to utility.

2. Group Sensitivity Labels

The creation of a mechanism by which the subjects and objects in a system could be reliably associated with work groups might make functionally trusted CSCW possible. The following definitions and conventions describe and clarify concepts and relationships which make group sensitivity labels possible.

a. *Definitions:*

(1) **Object.** An object is a passive entity in the system, for example, a data element.

(2) **Subject.** A subject is an active entity, human or non-human. Examples would be a data processing routine, and a human user.

(3) **Member.** A member is a human subject.

(4) **Sensitivity Level.** A sensitivity level (s_i) is an element of a partially ordered set $S = \{s_1, s_2, s_3, ..., s_n\}$, the sensitivity of the elements of S being ordered under the '<' operator; the sensitivity of s_1 < the sensitivity of s_2 < the sensitivity of s_3, etc. In an organization using a simple military model:
$S = \{Unclassified, Confidential, Secret, Top Secret\}$.

46

(5) **Compartment.** A compartment (c_i) is a container which can hold a grouping of objects of varying sensitivity levels. A compartment is also an element of the set of all compartments in an organization, $C = \{c_1, c_2, c_3, ..., c_p\}$.

(6) **Compartment List.** A compartment list (L_i) is a set of compartments: $L_i = \{c_1, c_2, c_3, ..., c_m\}$. A military example of a compartment list might be: $L_i = \{NATO, INTEL, CRYPTO, LOGISTICS\}$

(7) **Work Group.** A work group (g_x) is an arbitrary unordered set of j members:
$g_x = \{m_1, m_2, m_3, ..., m_j\}$.

(8) **Work Group List.** A work group list (G_i) is the set of all work groups in an organization:
$G = \{g_1, g_2, g_3, ..., g_k\}$.

b. Conventions

(1) **Security Domain.** The security domain (D) of a system is described by all possible pairings of all sensitivity levels and all compartments:
$D = S \times C$ (See subsection c below.)

(2) **Individual Security Domain.** An individual security domain d_i is a particular subset of D ($d_i \subset D$), a listing of all objects in D which individual i is authorized to access.

47

(3) **Group Security Domain.** A work group's security
domain (δ_A) is that subset of D listing all objects
in D which all members of working group A are
authorized to access: $\delta_A = d_1 \cap d_2 \cap d_3 \cap \ldots \cap d_j$,
where g_A has j members. Group security domains
will be subject to the following conditions:

- The sensitivity level of g_A will be no greater
  than the *lowest* sensitivity level of any
  member of g_A.

- The compartment list of g_A will be the least
  common subset of the compartment lists of all
  members of g_A: $L_{g_A} = L_{m_1} \cap L_{m_2} \cap L_{m_3} \cap \ldots \cap L_{m_j}$

c. *A Security Domain Example.*

In a hypothetical system with four sensitivity levels
and five compartments, the security domain (D) of the system
would be:

$$D = \{(s_4,c_1), (s_4,c_2), (s_4,c_3), (s_4,c_4), (s_4,c_5),$$
$$(s_3,c_1), (s_3,c_2), (s_3,c_3), (s_3,c_4), (s_3,c_5),$$
$$(s_2,c_1), (s_2,c_2), (s_2,c_3), (s_2,c_4), (s_2,c_5),$$
$$(s_1,c_1), (s_1,c_2), (s_1,c_3), (s_1,c_4), (s_1,c_5)\}$$

Suppose that four users of the system, all members of a work
group (g_A), have the following security access profiles:

Member	Sens.Level	Compartment Lists	Indiv. Sec. Domain
m_1	s_4	$L_{m_1} = \{c_1, c_2, c_3, c_4\}$	$d_1 = s_4 \times L_{m_1}$
m_2	s_4	$L_{m_2} = \{c_3, c_4, c_5\}$	$d_2 = s_4 \times L_{m_2}$
m_3	s_3	$L_{m_3} = \{c_1, c_2, c_3, c_4\}$	$d_3 = s_3 \times L_{m_3}$
m_4	s_3	$L_{m_4} = \{c_2, c_3, c_4, c_5\}$	$d_4 = s_3 \times L_{m_4}$

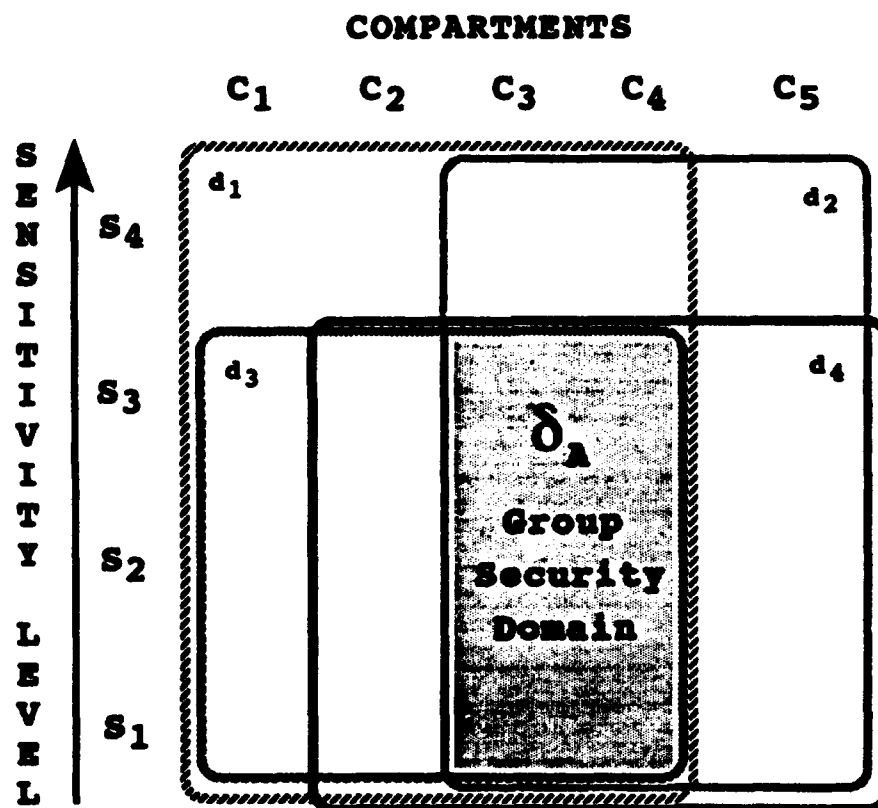Figure 2 pictorially represents the domain relationships described above.

Figure 2.   Individual and Group Security Domains
in a Hypothetical System.

A listing of the group security domain follows:

$$\delta_A = \{(s_3, c_3), (s_3, c_4),$$

$$(s_2, c_3), (s_2, c_4),$$

$$(s_1, c_3), (s_1, c_4)\}$$

d. Label Syntax

Under this proposed extended system, subject and object sensitivity labels (Λ) would have the following syntax: $\Lambda_i = (s_i, C_i)$. That is, every subject and object in the system will be stamped with a single sensitivity level and a compartment list specifying one or more authorized compartments.

(1) Subject Labels. Subjects in the system might have authorized access to one, a few, or many compartments. For example, the system's security kernel would grant an intelligent agent designed to conduct a context matching search access to any data base object stamped with a sensitivity label equal to or lower than the agent's. (Note that a subject who's compartment list is identical to the compartment list of a work group's security domain could, in a sense, "work for the group.")

(2) Object Labels. In an organization using FT-CSCW, system objects should probably be limited to single compartments. Multiple compartment labels which match group security domain compartment labels in a sense give an object a "group identity," but matching compartment lists do not necessarily guarantee the group *exclusive* access to the object. System users *not* members of the group may still have

matching compartment lists, and under many conditions, objects created within groups may *need* to be shared with *all* authorized subjects. If exclusive group rights *is* a requirement, a simple mechanism would be to create temporary exclusive compartments for each group.

e. *Group Security Profile*

Let the highest sensitivity level and the compartment list of each group be called the group's security profile. In our hypothetical example above, g_A's security profile would be: $(s_3, \{c_3, c_4\})$ Note that a group security profile is in the same format as a subject label, and in fact can act as a subject label template. Group security profiles could be incorporated in a system's operating system and the system could use a look-up table of the organizational work group list (G) and associated group security profiles to mediate the user interface.

How might the users of a hypothetical FT-CSCW system accomplish work? What might a user interface which accommodates varying individual and group security domains resemble, and how might it be used?

B. A HYPOTHETICAL USER INTERFACE

The following interface design is intended to illustrate how an individual user might accomplish work on a system organized around group work (and is not intended to be predictive of the future of sophisticated CSCW.) Note that to individual users the operations of the reference monitor underlying the TCB are largely *transparent*. As users "move"

from display to display, the subjects and objects available change if and when the group security domain changes. The underlying system security policy stipulates access control, FT-CSCW enforces the policy through the use of the group sensitivity label system discussed above.

1.   **The Home Display**

After log-on and authentication our hypothetical user would be presented with a "home" display showing all work groups of which the user is a member (Figure 3.)
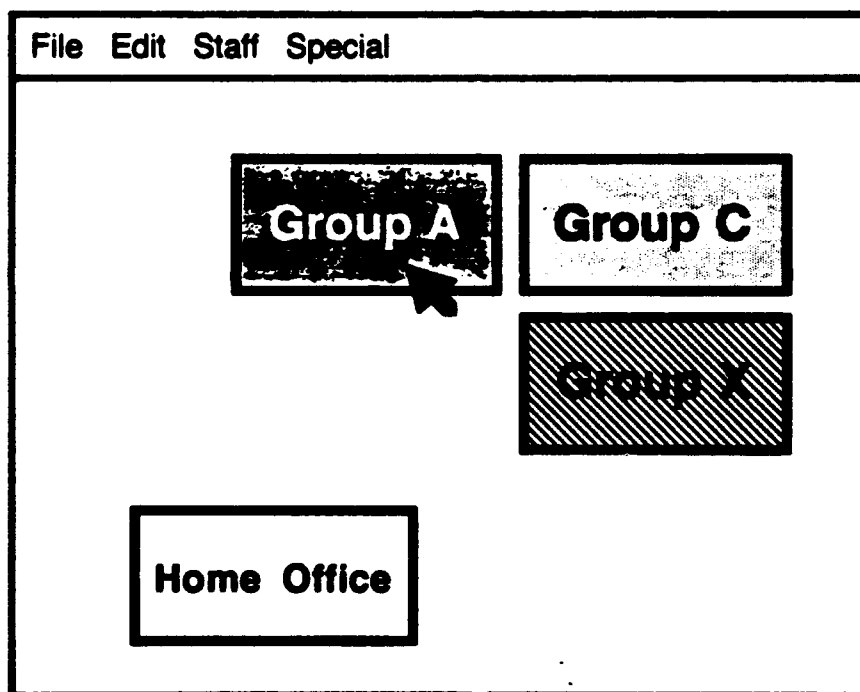

Figure 3.   The Home Display.

The menu bar and block marked "Home Office" would provide the user access to system utilities (including links,

52

coordinators, intelligent agents, and other sophisticated tools.) When accessed or invoked from the home display these subjects would all be stamped with sensitivity labels matching the user's personal security profile, (s_i, C_i).

While "in" the home office, our user would have access to objects and subjects which directly correspond to the user's information security profile, to the mandatory and discretionary access granted the user in accordance with the organization's security policy.

Let us suppose our user chooses to work as a member of group A. This would be accomplished by activating the Group A block (via pointing device, keyboard command, voice navigation, touch screen, or other means.) This would cause a "Group A display" to replace the home display.

2. The Group A Display

The interface of the Group A display is essentially similar to the home display; however, all subjects invoked from the group A display would be stamped with sensitivity labels identical to group A's security profile. Thus an intelligent agent invoked from the group A display (figure 4) would be able to conduct a key word search through all compartments listed in group A's compartment list and *no others.*
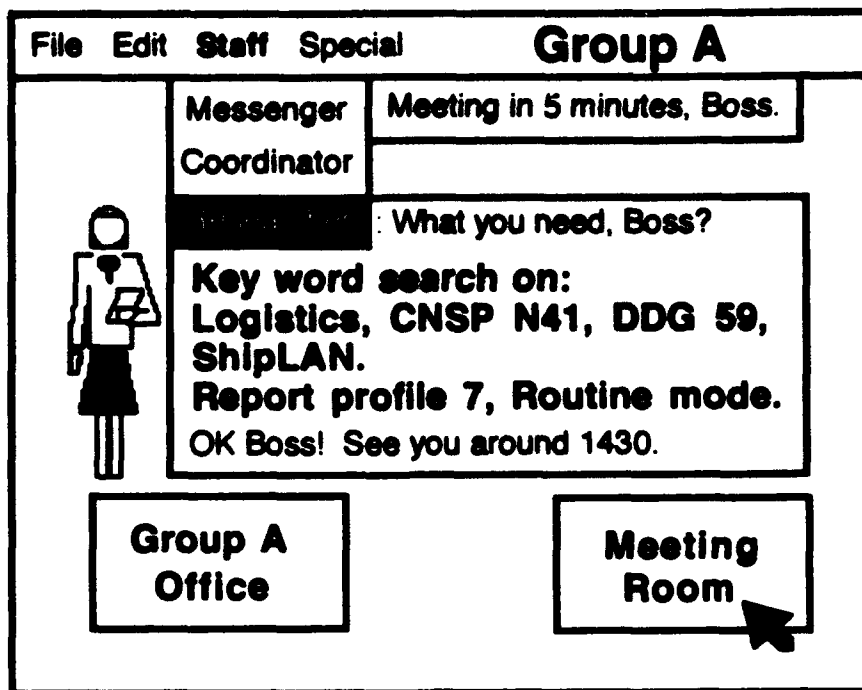
Figure 4. The Group A Display: An Agent is Instructed.

After instructing the intelligent agent, our hypothetical user chooses to attend a previously scheduled virtually co-located synchronous meeting by selecting the "meeting room" block (figure 5.)
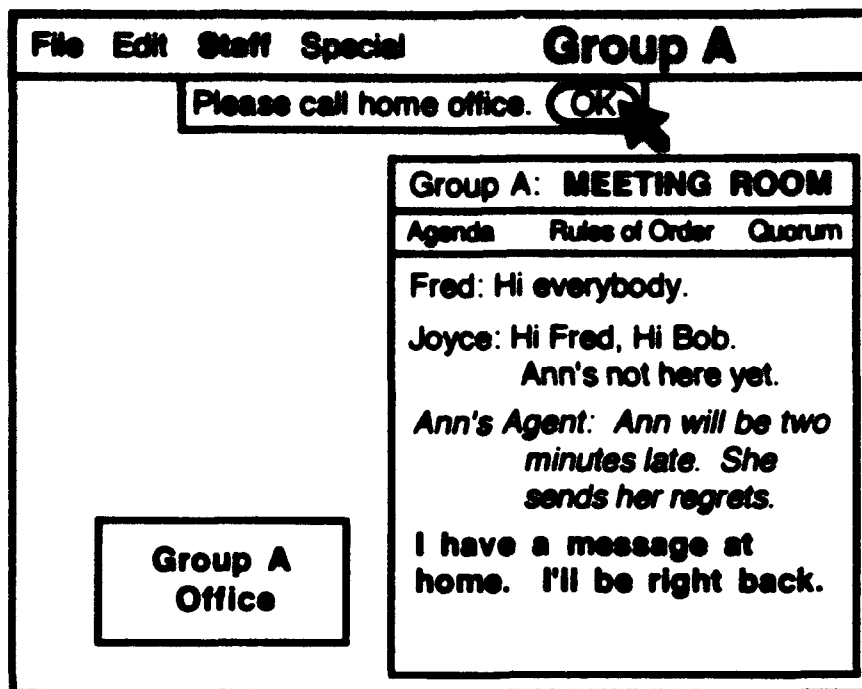
Figure 5. The Group A Display: In the Meeting Room.

The hypothetical conversation based dialogue in the "meeting room" is occurring in a shared window, one into which all group members are free to move authorized objects from their personal (and private) group desktops. A true shared window capable of supporting sophisticated CSCW would probably be rich in role-playing and normative cues, and might include voice, iconic symbols, full motion video or other devices. The above example is greatly simplified.

Note that a messenger agent has requested that our hypothetical user "please call home office." Any of several external events could have triggered this message; however, neither detailed nor differentiated messages can be passed into the Group A environment from outside. Anything other

than a simple generic message would constitute a potential covert channel into group A (or *from* group A into *another* group) and would be a violation of functional trust.

The development of a standard trusted interface would greatly simplify the multi-level security problem for the DoD. If such a standard were developed, COTS products which met DoD security requirements would be much easier for private software companies to develop, and DoD reliance on massive (and expensive) custom software systems might be greatly reduced. [Fact92] The conceptual GUI described above is presented in that spirit, but the author recognizes that formidable technical difficulties must be overcome before such a trusted interface could become a reality.

C. FUNCTIONALLY TRUSTED CSCW AT THE TACTICAL LEVEL

In addition to describing how work is accomplished at the individual level, it is also necessary to describe how FT-CSCW is accomplished at the organizational level, to describe how the activities of the group would accomplish the organization's routine tasks and strategic goals.

One possible mode of operation would be for FT-CSCW groups to "start low and work up." Work groups would begin work "constrained" by group security domains of low sensitivity and limited compartment access. After a group had accomplished all that was possible at a given level, low clearance members would leave the group (their personal memberships would be removed from the work group table,) causing the group ꜱ ꜱurity domain to "move up" in sensitivity

56

level. The group would now have new higher level objects for correlation and fusion into the group product. Eventually the group would reach the highest sensitivity level in the organization and no new objects would be available. At this point the group's work would be "complete" and the group product would be available for use or disposition by the organization's strategic apex.

Such a pattern of operations would "distill" the extensive object resource base of the organization into high value, high sensitivity objects. Unless the formal object declassification provision (and departure from the Bell-LaPadula model) discussed above were available, the group results could never be shared with low clearance members of the organization, and non-apical work groups would have to work without access to all the organization's information resources and in ignorance of past results.

The next chapter will address how functionally trusted CSCW might affect organizational structure and culture, and will discuss some serious problems and limitations inherent in the FT-CSCW concept.

V. FT—CSCW: EFFECTS AND PROBLEMS

This chapter will discuss several first order (efficiency) effects, second level (social) effects, and underlying problems which in the author's opinion will characterize, shape, and constrain organizations if they were to attempt to implement FT-CSCW.

It must be emphasized that FT-CSCW is a broad conceptual scheme, not a formal model. Some of the assertions or observations may seem somewhat audacious and unsubstantiated, but they are presented in the spirit of generalized discourse, not the presentation and defense of a realistic and/or precise model. (There will be further discussion of the role and rationale behind the FT-CSCW scheme in the final chapter.)

A. FIRST LEVEL EFFECTS

1. Sparse Group Domains

One of the promises of sophisticated CSCW is its capacity to marshal the resources of an organization simply by creating an environment of enhanced communication and collaboration. [Grud91] The author believes that if an organization has partitioned its information domain into multiple compartments, and for reasons of security is *unwilling* or *unable* to connect the information in these compartments, that organization will find that CSCW will not deliver as advertised. That is, if a group security domain is sparse (if it contains too few objects) the group will

find that it cannot accomplish its assigned tasks using sophisticated CSCW.

To the author, the irony is that organizations which protect and nurture "high valuable" and "important" information (such as Military Intelligence Activities) may watch organizations which process "low value" and "open" information enjoy orders of magnitude improvements in efficiency and quality, and will be unable to follow suit. If an organization is to experience the full benefits of sophisticated CSCW, group security domains must be made as large as possible. If a group's security domain is sparse, if it contains too few objects, the group will find that it cannot accomplish meaningful work.

2. The Breakdown of Compartmentation

In the author's opinion, the sparse domain effect discussed above may cause organizations to minimize the compartmentation of the information considered critical to their missions. That is, based on experience or the observation of successful FT-CSCW in other organizations, information domains will be realigned to improve the efficiency of CSCW groups.

Organizations which *must* handle information of the *highest* sensitivity will probably operate in an approximation of Dedicated Security Mode. Managers and analysts in such organizations would have access to open information resources imported from outside the organization, as well as non-open information solicited or submitted from other organizations.

Of course, under this Dedicated Mode arrangement, the single large compartment which would comprise the organization's security domain could still be guarded from unauthorized access. How (and whether) such organizations would share the results of their labor among "peer organizations" or simply pass the results to higher authority is problematical. The impact of one way information passage on the *quality* of the work of low level group results is also problematical.

3. Stratification

In organizations operating in the virtual System High mode discussed above, the residual high sensitivity information which for reasons of legal or military necessity *cannot* be shared with all members of the organization would probably be modularized into several small compartments, each containing only a few objects. These high sensitivity objects would be known (*from experience*) to be of limited value to *most* work groups. In the author's opinion, such organizations would ultimately become stratified into high sensitivity, full access groups and low sensitivity, limited access groups. In such organizations, mandatory access privileges would positively correlate with span of control. The strategic apex would have access to all information, "middle management" would have access to "most" information, and "production" level personnel would have access to "limited" but adequate information. (See figure 6.) Low-level groups would be monitored by upper level groups. Eventually low-level results would be passed to the upper-

level cadre, who would fuse the information not available to
the lower level. Next the results would be passed to the
apex, who would fuse any relevant top-level information. The
size of a member's security domain does not necessarily
correlate with the amount of information with which the
individual would contend. While the strategic apex of the
would have full access to all objects in the system,
filtering and fusion of information should balance the apical
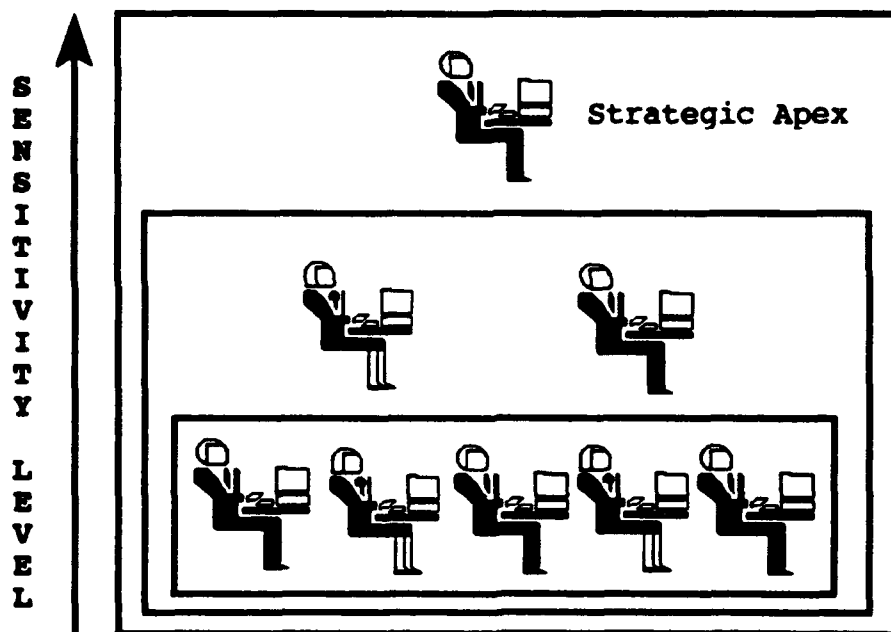information load.

Figure 6. Security Domains of the Different Structural
Levels of a Hypothetical Organization.

Although she approaches the issues with a group dynamic
perspective rather than one of computer security, Constance

61

Perin has also reached the conclusion that CSCW may sustain stratification in organizations. She states that even though Groupware is widely recognized as fostering an egalitarian and cooperative environment, there are social hierarchies within its use, and the traditional system of subordinates and superiors is reinforced rather than eliminated. [Peri91]

B.   SECOND LEVEL EFFECTS

The stratification of organizations into limited access and full access cadres would probably lead to several second level (social) effects.   In the author's opinion access stratification will probably reinforce social stratification. Access and status will become entrained. Apical cadres with full access will enjoy high status, while production-level cadres with limited access will enjoy lower status. Organizations subject to this stratification would probably tend towards mechanistic patterns of management and operating, even though organistic patterns might better suit the mission or challenges facing the group [Bola88].

Rothschild and Whitt state that knowledge diffusion is *crucial* if democratic organizations are to avoid monopolization of knowledge and "oligarchization." [Roth86] Kling states that conventional analyses of the effects of computer-based technologies on complex organizations which emphasize formal boundaries based on utilization of the resource (like the FT-CSCW model discussed above) fail to capture important social relationships which directly affect the development of the system.   Kling advocates the use of

62

"web models" (resource-dependency models) which explain how social leverage, the forces which promote smooth operation, and social settings influence system development [Klin87]. In the author's opinion, security based stratification reduces the value of the insights that might be gained from analysis using methods like Kling's, as any insights or alternative organizational structures suggested would probably run afoul of the organization's existing security policy.

Boland discusses several "information fantasies" which are common in IS research. Information is not structured data, the organization itself, power, intelligence, nor is it perfectible. The value of information lies in its *meaning*, in the result of *engagement* with the data. In this light, objects which are "protected" in exclusive compartments are, in fact, devalued [Bola87]. In an organization stratified by security requirements, this devaluation is minimal from the point of view of the strategic apex, but it is real, nevertheless. From Boland's perspective, *any* constraints on interconnectivity are devaluing.

Once again, the author perceives an emerging picture tinged with irony. CSCW promises a revolution in the work place, perhaps even the emergence of new structures and work cultures, and security requirements severely constrain if not veto the effects.

C. PROBLEMS

Numerous problem areas plague the FT-CSCW concept.

1. The Human Trust Problem Revisited

The most serious problem with the FT-CSCW concept is the Human Trust problem. *Functional trust is not Trust.* If an organization chooses to relax its information security standards in order to maximize interconnectivity, facilitate CSCW, or for any other reason, it must be understood that there is a price to be paid. If the value of a given object is perceived to reside in the maintenance of *absolute secrecy*, and if humans *are* part of the system (which is manifest) then functional trust is not enough. The richer the social interaction allowed by the system, the more sophisticated the conferencing, messaging, and meeting facilities, the greater the threat of covert channeling. From the point of view of absolute secrecy, the great power of CSCW is more than balanced by the great danger. In the author's opinion, *unequivocally highly sensitive information* (such as weapons launch codes or records of ongoing diplomatic negotiations) may never be allowed to be processed in other than formally Trusted Systems running in Dedicated Security Mode, and will only move from system to system via the cryptographic equivalent of diplomatic pouch.

Even if Trust is abandoned in favor of Functional Trust, other problems exist with the FT-CSCW concept.

2. Unstable Group Membership

A group's security domain is bounded by the least common level of sensitivity and the least common compartment access list of its members. Now suppose a group's membership is not stable. That is, suppose the turnover rate of a group's members is significant relative to the time-frame of overall group task accomplishment. Leaving members or new members might happen to have individual security domains which are critical constraints to the group domain. Therefore, without careful management, changes in group membership could cause the group domain to expand or contract. A group's members could report for work one day, find that a new member has joined the group and find that they no longer have access to all or part of the previous day's group work. The unstable membership problem would be ameliorated by the compartment breakdown effect discussed above. If an organization's compartmentation is minimal, changing memberships have minimal effect on group security domains. It is noteworthy that this is one more possible manifestation of the coincidence of *access* with *status*. Under FT-CSCW, apical cadre groups could not add low cadre individuals to their groups even if they wanted to, as the low cadre recruit would cause the apical security domain to collapse to low cadre levels. The only way low cadre individuals could join an apical work group would be through formal promotion.

3. Quality Improvement Circles

Related to the discussion immediately above is the problem of Quality Improvement Circles. In modern organizations, Quality Improvement Circles direct the resources of the organization towards process improvement by empowering traditionally low status members of the organization [Harr87]. In a stratified FT-CSCW organization, Quality Improvement Circles would find themselves restricted to the low access cadre group security domain. Now it may be the case that this is all the access the circle requires to accomplish its work, but how could the group *know* this? The low access limitation is not only contrary to the collaborative spirit of sophisticated CSCW [Grud91], it is also contrary to the spirit of Total Quality Improvement [Harr87].

4. Inter-Group CSCW

FT-CSCW between groups belonging to different organizations remains a problem. *Within* organizations, sensitivity labels would facilitate the operation of all forms of sophisticated CSCW: messaging, conferencing, co-authoring, augmentation, and even meeting room systems; however, as discussed previously, extensive coordination would be necessary to reconcile the sensitivity labels of one TCB with the sensitivity labels of another (assuming of course that both organizations were willing *or legally allowed* to share sufficient security policy information to make such coordination possible.)

In the author's opinion, inter-organizational CSCW may only be practical by the use of third-party meeting rooms, meeting rooms which are common facilities run my third-party TCB's. Such meeting rooms could be used by groups at different sensitivity levels. That is, Unclassified, Secret, or Top Secret meetings between the same organizations would be allowed; however, each organization would probably place restrictions on the objects their members would be allowed to bring to the meetings. "Cleared for meeting" compartments, compartments designed to contain objects the organization is willing to "risk" at external meetings, would probably be used. These third-party meeting rooms could be geographically co-located, locally remote, or fully remote, but from the point of view of TCB domains, they would be fully isolated. Figure 7 illustrates the relationships.

5. Visitors

How to handle outsiders is also a problem for organizations using FT-CSCW. Visitors to organizations would have to be granted fully integrated clearance before they could participate in CSCW or interact with work groups. One solution which occurs to the author would be to create visitor clearance profiles as a part of every work group. Outsiders invited to join groups would be classified according to the amount of access within the group security domain required for them to contribute, and granted the appropriate clearance package. Examples of visitor access packages might be "full-access" for visitors expected to act

temporarily as full members of the group and organization, and "limited-access" for vendors and consultants whose goals might not precisely coincide with the group and organization. Limited access visitors would probably be very temporary members of the group, as their highly restricted access would constrain the entire group as long as they were members.

It must be stressed that all of the effects and problems discussed above, like the FT-CSCW scheme itself, are presented in a broad, non-technical vein. It is the author's contention that the use of FT-CSCW will *predispose* an organization to stratification and the abandonment of compartmentation, but it will not inevitably *lead* to these effects.
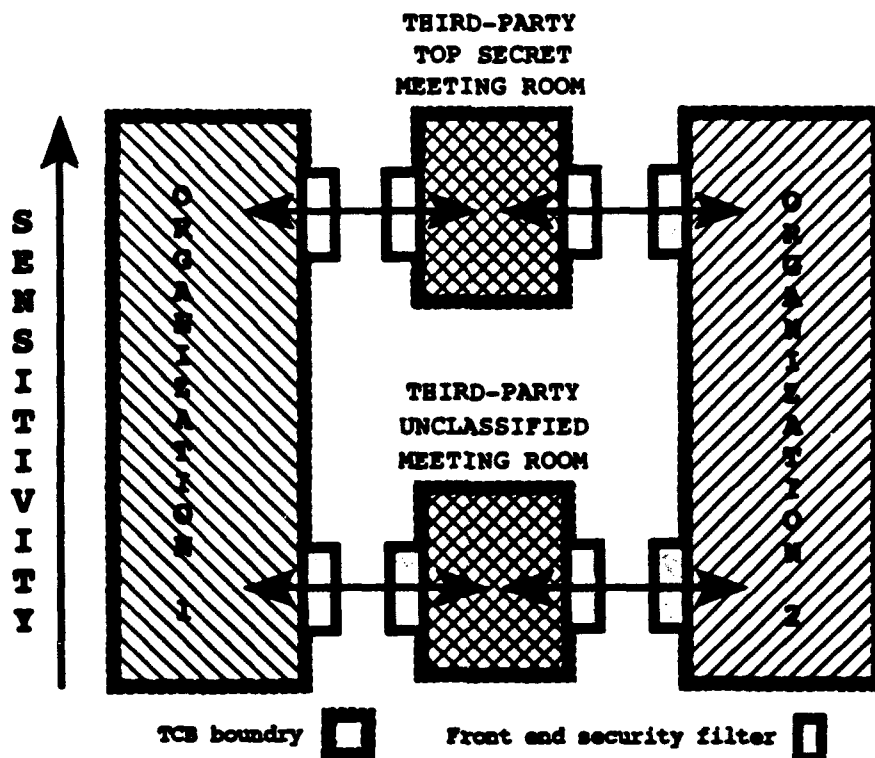

Figure 7. Two Organizations Using Third-Party Meeting Rooms.

The last chapter of this thesis will summarize my findings and make some final observations.

.

VI. CONCLUSIONS

In this thesis the author has attempted to describe in broad terms the future of Groupware and CSCW, to summarize the computer security requirements with which DoD and all other government organizations must comply, and to describe a broad scheme by which CSCW which complies with many (but not all) of these requirements might be accomplished (FT-CSCW), and finally to discuss some of the effects and problems which might accompany FT-CSCW.

In the author's opinion, broad conceptual schemes such as FT-CSCW are valuable to any field of endeavor as they help conceptualize the interactions of relevant variables, surface assumptions, and suggest areas which are being underemphasized or even neglected by current research. For example, Lee, Mansfield, and Sheth have developed a conceptual model which describes a control scheme for cooperative agents [Lee93]. The model involves the use of a system of Interactive Transactions (ITXs) which continually monitor and mediate individual user links to cooperative events such as multimedia conferences. Each user's ITX set attempts to optimize the user's participation in the cooperative event by determining the state of system resources relative to a set of fixed-point criteria. That is, each ITX monitors the system link and takes prescriptive action in accordance with preestablished criteria when the cooperative state deviates from the fixed-point.

70

The ITX scheme is similar to the FT-CSCW scheme in that both are broad, conceptual models intended to explore generalized relationships. It is also noteworthy that both are also concerned with computer security. FT-CSCW is concerned with the *secrecy* aspect, and ITX is concerned with the *system availability* aspect. In the author's opinion, this dichotomy of security interests is representative of CSCW related research. As was discussed earlier, research is occurring on a broad front from the highly technical to the broadly sociological, and many disparate, loosely related issues are involved. There is nothing "wrong" with this situation. All of the issues addressed in the literature are important, germane, and should be addressed. System reliability is a significant issue and the ITX scheme serves a valuable service by exploring the relationship of this issue to cooperative agents. In the same vein, the FT-CSCW scheme attempts to explore the relationship of information secrecy to CSCW.

Concerning the three aspects of computer security, data integrity, system reliability, and secrecy are clearly of interest to all users; but not all users broach all three aspects with equal emphasis. It is only natural that applications tailored to database management should emphasize data integrity and that applications tailored to communications should emphasize system reliability, but secrecy is not so much a matter of the design of any particular application as it is the use to which the application is put. Secrecy is the realm of information

management, not the realm of the physical management of 1s and 0s. It is the author's hope that this discussion of the security aspects of CSCW will acquaint some readers with security constraints as they impact DoD and some readers with CSCW and Groupware.

A. SUGGESTIONS FOR FUTURE RESEARCH

Several possible avenues for possible research in the security aspects of CSCW occur to the author.

1. A Formal FT-CSCW Model

The author has presented a broad informal scheme for FT-CSCW. As a follow-on project, a *formal mathematical model* of FT-CSCW should be developed which could be used to explore the *logical ramifications* of the extensions to the Bell-LaPadula proposed by the author. Such a model would be of greatest interest to that segment of researchers most concerned with Computer Security issues, but in the author's opinion is the necessary next step if the secrecy related security issues raised by this thesis are to be addressed by ...e CSCW/Groupware community.

2. A FT-CSCW Pilot Project

The Naval Postgraduate School should invest in the software and hardware to implement a broad based CSCW pilot program which would allow faculty and students to explore the full functionality of CSCW. Meeting rooms, message systems, co-authoring/argumentation systems, and conference systems

72

should be installed, and as far as is possible with current technology and COTS Groupware, integrated into a single system with a common interface. This NPS-CSCW System would be a valuable platform for addressing all aspects of CSCW/Groupware, from the highly technical issues which would probably be of greatest interest to the NPS Computer Science Faculty and Students, to the sociology/management issues which would probably be of greatest interest to the NPS Administrative Science Faculty and Students. Further, all security aspects could be examined: Secrecy, Integrity, and System Availability. Class projects and administrative work utilizing this NPS-CSCW system would serve instructional and operational purposes, while simultaneously providing an extensive and ongoing research environment for faculty and thesis students. For a reasonable investment, NPS could become the DoD leader in applied and theoretical CSCW.

3. FT-CSCW and C^4I^2

A further avenue of research would be to relate the issues discussed in this thesis *directly* to Command, Control, Communications, Computers, Intelligence, and Information Systems (C^4I^2) currently utilized by the DoD. This could serve as a means for relating highly specific DoD requirements and systems to the promise of sophisticated CSCW. Information Warfare (IW), Command and Control Warfare (CCW), and other C^4I^2 subdisciplines unfamiliar and somewhat esoteric to the civilian community could be related to the more "mundane" topics currently under discussion in the

73

CSCW/Groupware literature. Such C^4I^2/CSCW research might interest the NPS National Security Affairs Faculty and Students.

.

.

LIST OF REFERENCES

[Axsm92]   Axsmith, C., "E-Mail Privacy and the Law,"
           *Proceedings of the 15th National Computer Security
           Conference*, 1992.

[Bock92]   Bock, G., "Groupware: The Next Generation for
           Information Processing?," in "Groupware: Software
           for Computer-Supported Cooperative Work," IEEE
           Computer Society Press, Los Alamitos CA, 1992.

[Bola87]   Boland, R.J., Jr., "The In-formation of Information
           Systems," in "Critical issues in Information
           Systems Research," Edited by Boland, R.J., Jr. and
           Hirchheim, R.A., John Wiley & Sons Ltd., New York,
           1987.

[Bola88]   Boland, R.J. Jr. and Greenberg, R.H., "Metaphorical
           Structurng of Organizational Ambiguity," in
           "Managing Ambiguity and Change," Pondy, L.R.,
           Boland, R.J., Jr, and Thomas, H. Eds. John Wiley &
           Sons Ltd., New York, 1988.

[Carr92]   Carr, G.M., "Share and Share Alike," *LAN
           Technology*, v8, n12, Nov 1992.

[Caru91]   Caruso, D., "EuroPARC Explores 'Media Spaces":
           Audio-Video Networks Allows Colleagues to Work
           Together Effectively, Naturally," *Digital Media: A
           Seybold Report*, v1, n5, Oct 1991.

[Cast92]   Castagna, R., "Groupware: Sharing Work on a LAN,"
           PC Sources, v3, n1, Jan 1992.

[Chok92]   Chokhani, S., "Trusted Products Evaluation,"
           Communications of the ACM, v35, n7, Jul 1992.

[Cole92]   Cole and Nast-Cole, "A Primer on Group Dynamics for
           Groupware Developers," in "Groupware: Software for
           Computer-Supported Cooperative Work," IEEE Computer
           Society Press, Los Alamitos CA, 1992.

[Dunc92]   Duncan, T., "QED Office Offers Complete Groupware-
           and More: Modules Could Match Most Standalone
           Products," *LAN Times*, v9, n6, 6 Apr 1992.

[Elli91]   Ellis, C.A., Gibbs, S.J., and Rein, G.L.,
           "Groupware: Some Issues and Experiences,"
           Communications of the ACM, v34, n1, Jan 1991.

[Esko92]   Eskow, D., "Spies Like Us," *Corporate Computing*,
           v1, n5, Nov 1992.

[Fact92]   Factor, G. *et al.*, "The Need for a Multilevel
           Secure (MLS) Trusted User Interface," *Proceedings
           of the 15th National Computer Security Conference*,
           1992.

[FedC92]   "Federal Criteria for Information Technology
           Security, Vol. 1, Protection Profile Development,"
           Draft, NIST and NCSC, Dec 1992.

[Fran91]   Francik, E., "Putting Innovation to Work: Adoption
           Strategies for Multimedia Communication Systems."
           Communications of the ACM, v34, n12, Dec 1991.

[Grau92]   Graubart, R., "Operating System Support for Trusted
           Applications," *Proceedings of the 15th National
           Computer Security Conference*, 1992.

[Grud91]   Grudin, J., "CSCW Introduction," *Communications of
           the ACM*, v34, n12, Dec 1991.

[Harr87]   Harrington, H.J., "The Improvement Process, How
           America's Leading Companies Improve Quality,"
           McGraw-Hill Book Co., New York, 1987.

[Higg92]   "Groupware: Getting a Grip on Work-Group Computing;
           It's Hard to Pin Down the Definition," *PC Week*,
           v9, n43, 26 Oct 1992.

[INFOSEC] "Information and Personnel Security Program
           Regulation," OPNAVINST 5510.1 Series.

[Ishi91]   Ishii, H., "Toward an Open Shared Workspace:
           Computer and Video Fusion Approach of
           TeamWorkStation," Communications of the ACM, v34,
           n12, Dec 1991

[JaBk92]   "A Guide to Understanding Security Modeling in
           Trusted Systems," NCSC-TG-010, Ver. 1 (Jade Book),
           Oct 1992.

[Klin87]   Kling, R., "Defining the Boundries of Computing
           Across Complex Organizations," in "Critical issues
           in Information Systems Research," Edited by Boland,
           R.J., Jr. and Hirchheim, R.A., John Wiley & Sons
           Ltd., New York, 1987.

[Klin91]   "Cooperation, Coordination, and Control in
           Computer-Supported Work," *Communications of the
           ACM*, v34, n12, Dec 91.

[Kyng91]   Kyng, M., "Designing for Cooperation: Cooperating
           in Design," Communications of the ACM, v34, n 12,
           Dec 1992.

[Lee93]   Lee, K., Mansfield, W.H.Jr., Sheth, A.P., "A
           Framework for Controllong Cooperative Agents,"
           Computer, Jul 1993.

[Mads89]   Madsen, C.M., "Approaching Group Communications by
           Means of an Office Building Metaphor," *Proceedings
           of the First European Conference on CSCW*, Sep 1989.

[Mars92]   Marshak, R.T., "The Groupware Phenomenon: Does it
           Focus on the Proper Issues?," Patricia Seybold's
           Office Computing Report, v15, n1, Jan 1992.

[NAISSP]   "Department of the Navy Automated Information
           System Security Program," SECNAVINST 5239.2 Series.

[OrBk85]   "DoD Trusted Computer System Evaluation Criteria,"
           DoD 5200.28 STD (Orange Book), Dec 1985.

[Peri91]   Perin, C. "Electronic Social Fields in
           Bureaucracies," *Communications of the ACM, v34,
           n12*, Dec 1991.

[Pfle89]   Pfleeger, C.P., "Security in Computing," Prentice
           Hall, Englewood Cliffs, NJ, 1989.

[Pres92]   Preston, A., "As Use of Groupware Increases,
           Remote Access, Speed, and Security Emerge as
           Critical Issues," *PC Week*, v9, n43, Oct 26, 1992.

[Rayl92]   Rayl, E.W., "How Nantucket Installed and Used Lotus
           Notes," *Data Based Advisor*, v10, n8, Aug 1992.

[Ricc93]   Ricciuti, M., "Spy Proof Your Data!," *Datamation*,
           v39, n5, 1 Mar 1993.

[Rodd92]   Rodden T., and Blair, G., "Distributed Systems
           Support for Computer Supported Cooperative Work,"
           Computer Communications, v15, n8, 1992.

[Roth86]   Rothschild, J. and Whitt, J.A., "The Cooperative
           Workplace: Potentials and Dilemmas of
           Organizational Democracy and Participation,"
           Cambridge University Press Cambridge, 1986.

[Rudy92]   "Paramax Execs Now Meet 'Screen-to-Screen,'"
            Computing Canada, v18, n5, 2 Mar 1992.

[Ryme92]   Rymer, J.R., "Security Black Hole. (Distributed
            System Security is Not Being Addressed by Large
            Systems Vendors)," *Patricia Seybold's Network
            Monitor*, v7, n5, May 1992.

[Schn92]   Schneier, B., "Computer Security: Key Management
            Issue," *MacWEEK*, v6, n11, 16 Mar 1993.

[Spro91]   Sproull, L. and Kiesler, S., "Connections: New Ways
            of Working in the Networked Organization," The MIT
            Press, Cambridge MA, 1991.

[Sull92]   Sullivan, E., "Document Imaging Makes Linking,
            Annotating Notes Files Easier," PC Week, v9, n44,
            2 Nov 1992.

[Weis91]   Weiser, M., "The Computer for the 21st Century,"
            Scientific American, v265, n3, Sep 1991.

INITIAL DISTRIBUTION LIST